

What is Claimed is:

1. An authentication token which is normally
2 held by a user and, when the user is to use a use device
3 for executing predetermined processing in accordance
4 with authentication data of the user, connected to the
5 use device to perform user authentication on the basis
6 of biometrical information of the user, comprising:
7 a personal collation unit including a sensor
8 for detecting the biometrical information of the user
9 and outputting a detection result as sensing data, a
10 storage unit which stores in advance registered data to
11 be collated with the biometrical information of the user,
12 and a collation unit for collating the registered data
13 stored in said storage unit with the sensing data from
14 said sensor and outputting a collation result as
15 authentication data representing a user authentication
16 result; and
17 a communication unit for transmitting the
18 authentication data from said personal collation unit to
19 the use device as communication data,
20 wherein said personal collation unit and
21 communication unit are integrated.
2. A token according to claim 1, wherein
2 said storage unit further stores in advance
3 user information unique to the user, which is to be used

4 for processing in the use device, and
5 said collation unit outputs the authentication
6 data containing the user information read out from said
7 storage unit.

3. A token according to claim 1, further
2 comprising a protocol conversion unit for converting the
3 communication data from said communication unit into a
4 predetermined data format and transmitting the
5 communication data to the use device.

4. A token according to claim 1, further
2 comprising a radio unit for transmitting the
3 communication data from said communication unit to the
4 use device through a radio section.

5. A token according to claim 3, further
2 comprising a radio unit for transmitting the
3 communication data from said protocol conversion unit to
4 the use device through a radio section.

6. A token according to claim 1, further
2 comprising a battery for supplying power.

7. A token according to claim 6, wherein said
2 battery comprises a secondary battery charged by power
3 supply from the use device when said authentication

4 token is connected to the use device.

8. A token according to claim 1, wherein said
2 storage unit has, in addition to a storage area for
3 storing the registered data, at least one storage area
4 for storing another information.

9. A token according to claim 7, wherein said
2 at least one storage area for storing another
3 information includes a storage area for storing personal
4 information of the user and a storage area for storing
5 service information.

10. An authentication system for executing user
2 authentication, which is necessary for use of a use
3 device for executing predetermined processing, by using
4 biometrical information of a user, comprising:
5 an authentication token which is normally held
6 by the user and, when the user is to use said use device,
7 connected to said use device to perform user
8 authentication on the basis of the biometrical
9 information of the user,
10 said authentication token comprising
11 a personal collation unit including a sensor
12 for detecting the biometrical information of the user
13 and outputting a detection result as sensing data, a
14 storage unit which stores in advance registered data to

15 be collated with the biometrical information of the user,
16 and a collation unit for collating the registered data
17 stored in said storage unit with the sensing data from
18 said sensor and outputting a collation result
19 representing a user authentication result as
20 authentication data, and

21 a first communication unit for transmitting
22 the authentication data from said personal collation
23 unit to said use device as communication data,

24 said personal collation unit and communication
25 unit being integrated, and

26 said use device comprising

27 a second communication unit for receiving the
28 communication data transmitted from said authentication
29 token and outputting the data as the authentication data,
30 and

31 a processing unit for executing the
32 predetermined processing on the basis of the collation
33 result contained in the authentication data from said
34 second communication unit.

11. A system according to claim 10, wherein said
2 storage unit has a plurality of storage areas for
3 storing not only the registered information of the user
4 but also another information.

12. A system according to claim 10, wherein

10 the communication data to said second communication unit.

15. A system according to claim 13, wherein
2 said system further comprises a radio module
3 connected to said authentication token to transmit the
4 communication data from said data conversion module to
5 said use device through a radio section, and
6 said use device comprises a radio unit for
7 receiving the communication data transmitted from said
8 radio module through the radio section and outputting
9 the communication data to said second communication unit.

16. A system according to claim 10, wherein said
2 authentication token further comprises a battery for
3 supplying power into said authentication token.

17. A system according to claim 13, wherein said
2 data conversion module further comprises a battery for
3 supplying power into said data conversion module and
4 authentication token.

18. A system according to claim 14, wherein said
2 radio module further comprises a battery for supplying
3 power into said radio module and authentication token.

19. A system according to claim 16, wherein said
2 battery comprises a secondary battery charged by power

3 supply from said use device when said authentication
4 token is connected to said use device.

20. A token according to claim 1, wherein
2 said authentication token further comprises
3 another storage circuit for storing a password of said
4 authentication token and token identification
5 information for identifying said authentication token,
6 and
7 when the personal collation result indicates
8 that the collation is successful, said communication
9 unit transmits the password and token identification
10 information in said another storage circuit to said
11 service providing apparatus as the communication data.

21. An authentication system for executing user
2 authentication, which is necessary when a user is to use
3 a service providing apparatus for providing a
4 predetermined service, by using biometrical information
5 of the user, comprising:
6 an authentication token which is normally held
7 by the user and, when the user is to use said service
8 providing apparatus, connected to said service providing
9 apparatus to perform user authentication on the basis of
10 the biometrical information of the user,
11 said authentication token comprising a
12 personal collation unit for performing collation on the

13 basis of the biometrical information detected from the
14 user to check whether the user is an authentic user, a
15 storage circuit for storing a password of said
16 authentication token and token identification
17 information for identifying said authentication token,
18 and a first communication unit for, when a collation
19 result by said personal collation unit indicates that
20 collation is successful, transmitting the password and
21 token identification information in said storage circuit
22 to said service providing apparatus as communication
23 data, and

24 said service providing apparatus comprising a
25 second communication unit for receiving the
26 communication data from said authentication token, a
27 first database for storing the token identification
28 information and password of said authentication token in
29 advance in association with each other, a collation
30 circuit for collating the password contained in the
31 communication data with a password obtained from said
32 first database using the token identification
33 information as a key, and a processing unit for
34 providing the service to the user on the basis of a
35 collation result by said collation circuit.

22. A system according to claim 21, further
2 comprising a registration apparatus connected to said
3 service providing apparatus through a communication

4 network to register the token identification information
5 and password in said database in association with each
6 other.

23. A system according to claim 21, wherein
2 said service providing apparatus has a
3 password generation circuit for generating a new
4 password and transmitting the new password to said
5 authentication token through said second communication
6 unit and updating the password stored in said first
7 database, and
8 said first communication unit of said
9 authentication token updates the password stored in said
10 storage circuit by the new password received from said
11 service providing apparatus.

24. A system according to claim 21, wherein
2 said service providing apparatus has a storage
3 circuit for storing device identification information
4 for identifying said service providing apparatus, and
5 said second communication unit reads out the device
6 identification information from said storage circuit and
7 transmits the identification information to said
8 authentication token when said authentication token is
9 connected, and
10 said authentication token has a second
11 database for storing the password and the device

20 authentication token in advance in a first database in
21 association with each other, collates the password
22 contained in the communication data received from the
23 authentication token with a password obtained from the
24 first database using the token identification
25 information as a key, and provides the service to the
26 user on the basis of a collation result.

26. A method according to claim 25, wherein the
2 token identification information and password are
3 registered in the first database in association with
4 each other from a registration apparatus connected to
5 the service providing apparatus through a communication
6 network.

27. A method according to claim 25, wherein
2 the service providing apparatus causes a
3 password generation circuit to generate a new password,
4 transmits the new password to the authentication token
5 through the second communication unit, and updates the
6 password stored in the first database, and
7 the authentication token updates the password
8 stored in advance by the new password received from the
9 service providing apparatus.

28. A method according to claim 25, wherein
2 the service providing apparatus stores device

identification information for identifying the service providing apparatus in advance, and transmits the device identification information to the authentication token when the authentication token is connected, and the authentication token stores in advance the password and the device identification information for identifying the service providing apparatus in a second database in association with each other, and uses, as the password to be transmitted to the service providing apparatus, a password obtained from the second database using the device identification information received from the service providing apparatus as a key.

29. A recording medium which stores a program for causing a computer to execute an authentication procedure of executing user authentication, which is necessary when a user is to use a service providing apparatus for providing a predetermined service, between the service providing apparatus and an authentication token for executing the user authentication using biometrical information of the user,

said program comprising the steps of:

in the service providing apparatus, storing token identification information and a password of the authentication token in a first database in advance in association with each other;

in the authentication token, after collation

15 of the user based on the biometrical information
16 detected from the user, and when a collation result
17 indicates that collation is successful, receiving
18 communication data containing the password of the
19 authentication token and the token identification
20 information for identifying the authentication token,
21 which is transmitted for the authentication token;
22 collating the password contained in the
23 communication data with a password obtained from the
24 first database using the token identification
25 information as a key; and
26 providing the service to the user on the basis
27 of a collation result.

30. A medium according to claim 29, wherein said
2 program further comprises the step of, in the service
3 providing apparatus, registering the token
4 identification information and password in the first
5 database in association with each other from a
6 registration apparatus connected to the service
7 providing apparatus through a communication network.

31. A medium according to claim 29, wherein said
2 program further comprises the steps of:
3 in the service providing apparatus, causing a
4 password generation circuit to generate a new password;
5 transmitting the new password to the

6 authentication token through the second communication
7 unit so as to update the password stored in the
8 authentication token in advance; and
9 updating the password stored in the first
10 database by the new password.

32. A medium according to claim 29, wherein said
2 program further comprises the steps of:
3 in the service providing apparatus, storing
4 device identification information for identifying the
5 service providing apparatus in advance; and
6 transmitting the device identification
7 information to the authentication token when the
8 authentication token is connected so as to store the
9 password and the device identification information used
10 to identify the service providing apparatus in the
11 authentication token in a second database in association
12 with each other, and searching the second database for a
13 password using the device identification information
14 received from the service providing apparatus as a key
15 as the password to be transmitted to the service
16 providing apparatus.

33. A program for causing a computer to execute
2 an authentication procedure of executing user
3 authentication, which is necessary when a user is to use
4 a service providing apparatus for providing a

5 predetermined service, between the service providing
6 apparatus and an authentication token for executing the
7 user authentication using biometrical information of the
8 user,

9 said program causing the computer to execute
10 the steps of:

11 in the service providing apparatus, storing
12 token identification information and a password of the
13 authentication token in a first database in advance in
14 association with each other;

15 in the authentication token, after collation
16 of the user based on the biometrical information
17 detected from the user, and when a collation result
18 indicates that collation is successful, receiving
19 communication data containing the password of the
20 authentication token and the token identification
21 information for identifying the authentication token,
22 which is transmitted for the authentication token;

23 collating the password contained in the
24 communication data with a password obtained from the
25 first database using the token identification
26 information as a key; and

27 providing the service to the user on the basis
28 of a collation result.

34. A program according to claim 33, further
2 comprising the step of, in the service providing

3 apparatus, registering the token identification
4 information and password in the first database in
5 association with each other from a registration
6 apparatus connected to the service providing apparatus
7 through a communication network.

35. A program according to claim 33, further
2 comprising the steps of:
3 in the service providing apparatus, causing a
4 password generation circuit to generate a new password;
5 transmitting the new password to the
6 authentication token through the second communication
7 unit so as to update the password stored in the
8 authentication token in advance; and
9 updating the password stored in the first
10 database by the new password.

36. A program according to claim 33, further
2 comprising the steps of:
3 in the service providing apparatus, storing
4 device identification information for identifying the
5 service providing apparatus in advance; and
6 transmitting the device identification
7 information to the authentication token when the
8 authentication token is connected so as to store the
9 password and the device identification information used
10 to identify the service providing apparatus in the

11 authentication token in a second database in association
12 with each other, and searching the second database for a
13 password using the device identification information
14 received from the service providing apparatus as a key
15 as the password to be transmitted to the service
16 providing apparatus.

37. A biometrical information authentication
2 storage which locks or unlocks a door of a main body in
3 storing an article in the main body or taking out the
4 article stored in the main body, and also unlocks the
5 door on the basis of authentication of biometrical
6 information of a user, comprising:
7 drive means for locking/unlocking the door;
8 storage means for storing the biometrical
9 information of the user; and
10 processing means for controlling said drive
11 means to unlock the door on the basis of matching
12 between stored information in said storage means and
13 detected information from a sensor for detecting the
14 biometrical information of the user.

38. A storage according to claim 37, wherein
2 said storage means stores a fingerprint image
3 of the user as the biometrical information, and
4 said processing means controls said drive
5 means to unlock the door on the basis of matching

7 storing the password in said storage means, transmitting
8 the password to the fingerprint authentication token,
9 and causing the fingerprint authentication token to
10 store the password, and

11 unlock means for controlling said drive means
12 to unlock the door when a password based on matching
13 between a registered fingerprint image and the
14 fingerprint image detected by the sensor and output from
15 the fingerprint authentication token is received in
16 taking out the article stored in the main body, and the
17 received password matches the password in said storage
18 means.

41. A storage according to claim 38, wherein
2 said processing means comprises
3 lock means for, when a password based on
4 matching between a registered fingerprint image and the
5 fingerprint image detected by the sensor and output from
6 the fingerprint authentication token is received in
7 storing the article in the main body, controlling said
8 drive means to lock the door, and storing the received
9 password in said storage means, and
10 unlock means for controlling said drive means
11 to unlock the door when the password based on matching
12 between the registered fingerprint image and the
13 fingerprint image detected by the sensor and output from
14 the fingerprint authentication token is received in

15 taking out the article stored in the main body, and the
16 received password matches the password in said storage
17 means.

42. A storage according to claim 38, wherein
2 said storage further comprises
3 a plurality of storage sections capable of
4 independently storing articles and having corresponding
5 doors,
6 designation means for designating one of the
7 plurality of doors, and
8 display means for displaying a number of the
9 door, and
10 said processing means comprises
11 first display control means for, when a
12 corresponding door is closed in storing an article in a
13 storage section, displaying the number of the door on
14 said display means,
15 lock means for, when the door number displayed
16 on said display means is designated by said designation
17 means, and the fingerprint authentication token is
18 inserted into the main body, controlling said drive
19 means to lock the door, generating a password, storing
20 the password and the door number in said storage means,
21 transmitting the password and the door number to the
22 fingerprint authentication token, and causing the
23 fingerprint authentication token to store the password

0955770.05101

24 and the door number,

25 second display control means for, when the
26 fingerprint authentication token is inserted into the
27 main body in taking out the article stored in said
28 storage section, displaying the door number stored in
29 the fingerprint authentication token on said display
30 means, and

31 unlock means for controlling said drive means
32 to unlock the door when the door number displayed on
33 said display means is designated by said designation
34 means, and a password based on matching between a
35 registered fingerprint image and the fingerprint image
36 detected by the sensor and output from the fingerprint
37 authentication token is received, and the received
38 password matches the password in said storage means.

43. A storage according to claim 37, wherein
2 said storage further comprises check means for
3 checking coins of a predetermined amount, which are put
4 in by the user in storing the article, and
5 when said check means checks that the coins of
6 the predetermined amount are put in, said processing
7 means controls said drive means to lock the door.

44. A lock/unlock method for a biometrical
2 information authentication storage which locks or
3 unlocks a door of a main body in storing an article in

4 the main body or taking out the article stored in the
5 main body, and also unlocks the door on the basis of
6 authentication of biometrical information of a user,
7 comprising:

8 the first step of unlocking the door on the
9 basis of matching between stored information stored in
10 storage means in advance and detected information from a
11 sensor for detecting the biometrical information of the
12 user.

45. A method according to claim 44, wherein

2 the storage means stores a fingerprint image
3 of the user as the biometrical information, and

4 processing in the first step comprises the

5 second step of unlocking the door on the basis of

6 matching between the stored information in the storage

7 means and the fingerprint image from a fingerprint

8 authentication token having the sensor for detecting the

9 fingerprint image of the user as the biometrical

10 information.

46. A method according to claim 45, wherein

2 processing in the second step comprises

3 the third step of, when the fingerprint image

4 of the user, which is transmitted from the fingerprint

5 authentication token, is received in storing the article

6 in the main body, locking the door and storing the

0952720.05104

7 received fingerprint image in the storage means, and
8 the fourth step of unlocking the door when the
9 fingerprint image of the user, which is transmitted from
10 the fingerprint authentication token, is received in
11 taking out the article stored in the main body, and the
12 received fingerprint image matches the stored
13 information in the storage means.

47. A method according to claim 45, wherein
2 processing in the second step comprises
3 the fifth step of, when the fingerprint
4 authentication token is inserted into the main body in
5 storing the article in the main body, locking the door,
6 generating a password, storing the password in the
7 storage means, transmitting the password to the
8 fingerprint authentication token, and causing the
9 fingerprint authentication token to store the password,
10 and
11 the sixth step of unlocking the door when a
12 password based on matching between a registered
13 fingerprint image and the fingerprint image detected by
14 the sensor and output from the fingerprint
15 authentication token is received in taking out the
16 article stored in the main body, and the received
17 password matches the password in the storage means.

48. A method according to claim 45, wherein

2 processing in the second step comprises
3 the seventh step of, when a password based on
4 matching between a registered fingerprint image and the
5 fingerprint image detected by the sensor and output from
6 the fingerprint authentication token is received in
7 storing the article in the main body, locking the door,
8 and storing the received password in the storage means,
9 and

10 the eighth step of unlocking the door when the
11 password based on matching between the registered
12 fingerprint image and the fingerprint image detected by
13 the sensor and output from the fingerprint
14 authentication token is received in taking out the
15 article stored in the main body, and the received
16 password matches the password in the storage means.

49. A method according to claim 45, wherein

2 the storage further comprises a plurality of
3 storage sections capable of independently storing
4 articles and having corresponding doors, and

5 processing in the second step comprises
6 the ninth step of, when a corresponding door
7 is closed in storing an article in a storage section,
8 displaying a number of the door,

9 the 10th step of, when the door number
10 displayed on the basis of processing in the ninth step
11 is designated, and the fingerprint authentication token

12 is inserted into the main body, locking the door,
13 generating a password, storing the password and the door
14 number in the storage means, transmitting the password
15 and the door number to the fingerprint authentication
16 token, and causing the fingerprint authentication token
17 to store the password and the door number,

18 the 11th step of, when the fingerprint
19 authentication token is inserted into the main body in
20 taking out the article stored in the storage section,
21 displaying the door number stored in the fingerprint
22 authentication token, and

23 the 12th step of unlocking the door when the
24 door number displayed on the basis of processing in the
25 11th step is designated, and a password based on
26 matching between a registered fingerprint image and the
27 fingerprint image detected by the sensor and output from
28 the fingerprint authentication token is received, and
29 the received password matches the password in the
30 storage means.

50. A method according to claim 45, wherein
2 the method further comprises the 13th step of
3 checking coins of a predetermined amount, which are put
4 in by the user in storing the article, and
5 processing in the first step comprises the
6 14th step of locking the door when that the coins of the
7 predetermined amount are put in is checked on the basis

8 of processing in the 13th step.

51. A gate opening/closing system for

2 opening/closing an entrance gate for a site, comprising:

3 an authentication token for authenticating a

4 user on the basis of biometrical information of the

5 user;

6 a database for storing identification

7 information of the user when the user prepays an

8 admission to the site; and

9 control means for, when said authentication

10 token authenticates that the user is an authentic user,

11 and the identification information of the user, which is

12 stored in said authentication token in advance, is

13 output from said authentication token at the time of

14 entrance of the user to the site, receiving the

15 identification information, and when the received

16 identification information has been stored in said

17 database, opening the entrance gate.

52. A gate opening/closing system for

2 opening/closing an entrance gate for a site, comprising:

3 information transmission/reception means for

4 transmitting/receiving information to/from an

5 authentication token which stores identification

6 information of a user;

7 a database for storing the identification

0383270.051301

8 information of the user when the user prepays an
9 admission to the site; and
10 control means for opening the entrance gate
11 when said authentication token authenticates that the
12 user is an authentic user on the basis of biometrical
13 information of the user, the identification information
14 of the user, which is output from said authentication
15 token, is received by said information
16 transmission/reception means at the time of entrance of
17 the user to the site, and the received identification
18 information has been stored in said database.

53. A system according to claim 51, wherein
2 said authentication token is a fingerprint
3 authentication token for authenticating the user on the
4 basis of fingerprint information of the user, and
5 comprises
6 storage means for storing the fingerprint
7 information of the user,
8 a fingerprint sensor for detecting a
9 fingerprint of the user, and
10 processing means for authenticating the user
11 as the authentic user on the basis of matching between
12 detected information from said fingerprint sensor and
13 stored information in said storage means.

54. A system according to claim 52, wherein

2 said authentication token is a fingerprint
3 authentication token for authenticating the user on the
4 basis of fingerprint information of the user, and
5 comprises
6 storage means for storing the fingerprint
7 information of the user,
8 a fingerprint sensor for detecting a
9 fingerprint of the user, and
10 processing means for authenticating the user
11 as the authentic user on the basis of matching between
12 detected information from said fingerprint sensor and
13 stored information in said storage means.

55. A system according to claim 51, further
2 comprising identification information assignment means
3 for, when said fingerprint authentication token is
4 inserted, and the user prepays the admission to the site,
5 generating a password and causing said fingerprint
6 authentication token to store the password as the
7 identification information, and transmitting the
8 password to said database and causing said database to
9 store the password as the identification information of
10 the user.

56. A system according to claim 52, further
2 comprising identification information assignment means
3 for, when said fingerprint authentication token is

03552770-051103

4 inserted, and the user prepays the admission to the site,
5 generating a password and causing said fingerprint
6 authentication token to store the password as the
7 identification information, and transmitting the
8 password to said database and causing said database to
9 store the password as the identification information of
10 the user.

57. A system according to claim 51, wherein
2 said fingerprint authentication token stores
3 an identification number of the user as the
4 identification information in advance, and
5 said system further comprises identification
6 information assignment means for, when said fingerprint
7 authentication token is inserted, and the user prepays
8 the admission to the site, reading the identification
9 information from the fingerprint authentication token,
10 transmitting the identification information to said
11 database, and causing said database to store the
12 identification information as the identification
13 information of the user.

58. A system according to claim 52, wherein
2 said fingerprint authentication token stores
3 an identification number of the user as the
4 identification information in advance, and
5 said system further comprises identification

08553770.051104

6 information assignment means for, when said fingerprint
7 authentication token is inserted, and the user prepays
8 the admission to the site, reading the identification
9 information from the fingerprint authentication token,
10 transmitting the identification information to said
11 database, and causing said database to store the
12 identification information as the identification
13 information of the user.

59. A system according to claim 51, further
2 comprising
3 transmission means for converting
4 identification information added to said authentication
5 token and output from said authentication token into a
6 radio signal or infrared signal and transmitting the
7 signal, and
8 reception means, arranged near the entrance
9 gate, for, upon receiving the radio signal or infrared
10 signal transmitted by said transmission means, sending
11 the identification information contained in the received
12 radio signal or infrared signal to said control means.

60. A system according to claim 52, further
2 comprising
3 transmission means for converting
4 identification information added to said authentication
5 token and output from said authentication token into a

6 radio signal or infrared signal and transmitting the
7 signal, and
8 reception means, arranged near the entrance
9 gate, for, upon receiving the radio signal or infrared
10 signal transmitted by said transmission means, sending
11 the identification information contained in the received
12 radio signal or infrared signal to said control means.

61. A biometrical information authentication
2 automatic teller machine for providing, to a user, a
3 service including deposit/withdrawal of cash for the
4 user on the basis of authentication of biometrical
5 information of the user, comprising:
6 a biometrical information authentication token
7 for authenticating the user on the basis of the
8 biometrical information of the user,
9 said biometrical information authentication
10 token comprising
11 storage means for storing the biometrical
12 information of the user,
13 a sensor for detecting the biometrical
14 information of the user, and
15 processing means for outputting control
16 information on the basis of matching between detected
17 information from said sensor and stored information in
18 said storage means, and
19 said biometrical information authentication

09853770.051101

20 automatic teller machine comprising service providing
21 means for providing the service to the user on the basis
22 of the control information from said processing means.

62. A machine according to claim 61, wherein

2 said machine further comprises a database
3 which stores an outstanding balance corresponding to an
4 account number of the user in advance,

5 said storage means of said biometrical
6 information authentication token stores the account
7 number of the user,

8 said processing means outputs the account
9 number in said storage means as the control information
10 on the basis of matching between the detected
11 information from said sensor and the stored information
12 in said storage means, and

13 said service providing means comprises
14 acquisition means for, upon receiving the
15 account number from said processing means, acquiring the
16 outstanding balance corresponding to the received
17 account number from said database,

18 withdrawal means for withdrawing cash
19 corresponding to predetermined operation by the user
20 from the outstanding balance acquired by said
21 acquisition means, and

22 outstanding balance recording means for
23 subtracting an amount withdrawn by said withdrawal means

24 from the outstanding balance acquired by said
25 acquisition means and storing a new outstanding balance
26 in said database.

63. A machine according to claim 61, wherein
2 said machine further comprises a database
3 which stores an outstanding balance corresponding to an
4 account number of the user in advance,
5 said storage means of said biometrical
6 information authentication token stores the account
7 number of the user,
8 said processing means outputs the account
9 number in said storage means as the control information
10 on the basis of matching between the detected
11 information from said sensor and the stored information
12 in said storage means, and
13 said service providing means comprises
14 acquisition means for, upon receiving the
15 account number from said processing means, acquiring the
16 outstanding balance corresponding to the received
17 account number from said database, and
18 outstanding balance recording means for adding
19 an amount deposited by the user to the outstanding
20 balance acquired by said acquisition means and storing a
21 new outstanding balance in said database.

64. A biometrical information authentication

2 automatic teller machine for providing, to a user, a
 3 service including deposit/withdrawal of cash for the
 4 user on the basis of authentication of biometrical
 5 information of the user, comprising:
 6 information transmission/reception means for
 7 transmitting/receiving information to/from a biometrical
 8 information authentication token for authenticating the
 9 user on the basis of comparison/collation between
 10 biometrical information stored in storage means and the
 11 biometrical information of the user, which is detected
 12 by a sensor; and
 13 service providing means for, when said
 14 information transmission/reception means receives
 15 control information output from the biometrical
 16 information authentication token on the basis of
 17 matching between detected information from the sensor
 18 and the biometrical information in the storage means,
 19 providing the service to the user on the basis of the
 20 received control information.

65. A machine according to claim 64, wherein
 2 said machine further comprises a database
 3 which stores an outstanding balance corresponding to an
 4 account number of the user in advance,
 5 the storage means of the biometrical
 6 information authentication token stores the account
 7 number of the user, and

8 said service providing means comprises
9 acquisition means for, when said information
10 transmission/reception means receives the account number
11 output from the biometrical information authentication
12 token as the control information on the basis of
13 matching between the detected information from the
14 sensor and the biometrical information in the storage
15 means, acquiring the outstanding balance corresponding
16 to the received account number from said database,
17 withdrawal means for withdrawing cash
18 corresponding to predetermined operation by the user
19 from the outstanding balance acquired by said
20 acquisition means, and
21 outstanding balance recording means for
22 subtracting an amount withdrawn by said withdrawal means
23 from the outstanding balance acquired by said
24 acquisition means and storing a new outstanding balance
25 in said database.

66. A machine according to claim 64, wherein
2 said machine further comprises a database
3 which stores an outstanding balance corresponding to an
4 account number of the user in advance,
5 the storage means of the biometrical
6 information authentication token stores the account
7 number of the user, and
8 said service providing means comprises

9 acquisition means for, when said information
10 transmission/reception means receives the account number
11 output from the biometrical information authentication
12 token as the control information on the basis of
13 matching between the detected information from the
14 sensor and the biometrical information in the storage
15 means, acquiring the outstanding balance corresponding
16 to the received account number from said database, and
17 outstanding balance recording means for adding
18 an amount deposited by the user to the outstanding
19 balance acquired by said acquisition means and storing a
20 new outstanding balance in said database.

67. A machine according to claim 61, wherein
2 when a passbook of the user is inserted, said
3 outstanding balance recording means records information
4 including the outstanding balance on the passbook.

68. A machine according to claim 64, wherein
2 when a passbook of the user is inserted, said
3 outstanding balance recording means records information
4 including the outstanding balance on the passbook.

69. A machine according to claim 61, wherein
2 said storage means stores a fingerprint image
3 of the user as the biometrical information,
4 said sensor detects the fingerprint image of

5 the user as the biometrical information, and
6 said processing means or biometrical
7 information authentication token outputs the control
8 information on the basis of matching between the
9 fingerprint image detected by said sensor and the
10 fingerprint image in said storage means.

0853770 051101
70. A machine according to claim 69, wherein
2 the storage means stores a fingerprint image
3 of the user as the biometrical information,
4 the sensor detects the fingerprint image of
5 the user as the biometrical information, and
6 said processing means or biometrical
7 information authentication token outputs the control
8 information on the basis of matching between the
9 fingerprint image detected by the sensor and the
10 fingerprint image in the storage means.

71. A portable terminal system comprising a
2 portable terminal device and a biometrical
3 authentication device,
4 said biometrical authentication device
5 comprising
6 biometrical information read means for reading
7 biometrical information of a user who holds said
8 biometrical authentication device,
9 first storage means for storing biometrical

10 information of an authentic user registered in advance
 11 and personal information of the authentic user, and
 12 a first processing unit for performing
 13 personal authentication by collating the biometrical
 14 information read by said biometrical information read
 15 means with the biometrical information of the authentic
 16 user stored in said first storage means, and only when
 17 an authentication result represents that collation is
 18 successful, transmitting the personal information stored
 19 in said first storage means to said portable terminal
 20 device, and
 21 said portable terminal device comprising
 22 second storage means for storing the personal
 23 information transmitted from said biometrical
 24 authentication device, and
 25 second processing means for executing
 26 communication processing or data processing using the
 27 personal information stored in said second storage means.

72. A portable terminal system comprising a
 2 portable terminal device and a biometrical
 3 authentication device,
 4 said biometrical authentication device
 5 comprising
 6 biometrical information read means for reading
 7 biometrical information of a user who holds said
 8 biometrical authentication device,

9 first storage means for storing biometrical
10 information of an authentic user registered in advance
11 and service information necessary for the authentic user
12 to receive a service, and

13 a first processing unit for performing
14 personal authentication by collating the biometrical
15 information read by said biometrical information read
16 means with the biometrical information of the authentic
17 user stored in said first storage means, and only when
18 an authentication result represents that collation is
19 successful, transmitting the service information stored
20 in said first storage means to said portable terminal
21 device, and

22 said portable terminal device comprising
23 second storage means for storing the service
24 information transmitted from said biometrical
25 authentication device, and

26 second processing means for executing
27 communication processing or data processing using the
28 service information stored in said second storage means.

73. A system according to claim 71, wherein
2 the personal information contains a personal
3 identification number of the authentic user, and
4 after the personal information is stored in
5 said second storage means, said second processing means
6 of said portable terminal device is connected to a

7 network using the personal identification number
8 contained in the personal information.

74. A system according to claim 72, wherein
2 the service information contains a password
3 used to log in to a web site, and
4 after the service information is stored in
5 said second storage means, said second processing means
6 of said portable terminal device acquires, from the
7 service information, a password corresponding to a web
8 site accessed through a network and transmits the
9 acquired password to the accessed web site.

75. A biometrical authentication device
2 comprising:
3 biometrical information read means for reading
4 biometrical information of a user who holds said device;
5 storage means for storing biometrical
6 information of an authentic user registered in advance
7 and personal information of the authentic user; and
8 a processing unit for performing personal
9 authentication by collating the biometrical information
10 read by said biometrical information read means with the
11 biometrical information of the authentic user stored in
12 said storage means, and only when an authentication
13 result represents that collation is successful,
14 transmitting the personal information stored in said

20 device which does not hold the service information,
21 thereby allowing communication processing or data
22 processing using the service information.

77. A device according to claim 75, wherein the
2 personal information contains a personal identification
3 number of the authentic user, which is necessary to
4 connect the portable terminal device to a network.

78. A device according to claim 76, wherein the
2 service information contains a password used to log in
3 to a web site from the portable terminal device through
4 a network.

79. A portable terminal device comprising:
2 storage means for receiving personal
3 information of an authentic user from a biometrical
4 authentication device and storing the personal
5 information, the biometrical authentication device
6 executing personal authentication using biometrical
7 information of a user, and transmitting the personal
8 information of the authentic user only when an
9 authentication result indicates that collation is
10 successful; and
11 processing means for executing communication
12 processing or data processing using the personal
13 information stored in said storage means,

14 wherein the communication processing or data
15 processing using the personal information is executed
16 only when the personal information stored in the
17 biometrical authentication device is received.

80. A portable terminal device comprising:
2 storage means for receiving service
3 information necessary for an authentic user to receive a
4 service from a biometrical authentication device and
5 storing the service information, the biometrical
6 authentication device executing personal authentication
7 using biometrical information of a user, and
8 transmitting the service information only when an
9 authentication result indicates that collation is
10 successful; and

11 processing means for executing communication
12 processing or data processing using the service
13 information stored in said storage means,

14 wherein the communication processing or data
15 processing using the service information is executed
16 only when the service information stored in the
17 biometrical authentication device is received.

81. A device according to claim 79, wherein
2 the personal information contains a personal
3 identification number of the authentic user, and
4 after the personal information is stored in

5 said storage means, said processing means of said
6 portable terminal device is connected to a network using
7 the personal identification number contained in the
8 personal information.

82. A device according to claim 80, wherein
2 the service information contains a password
3 used to log in to a web site, and
4 after the service information is stored in
5 said storage means, said processing means of said
6 portable terminal device acquires, from the service
7 information, a password corresponding to a web site
8 accessed through a network and transmits the acquired
9 password to the accessed web site.

83. A token according to claim 1, wherein
2 said token further comprises an encryption
3 circuit for encrypting data generated from the
4 authentication data and dynamic information generated by
5 the use device and transmitted using a key registered in
6 advance, and
7 said communication circuit transmits to the
8 use device encrypted data generated by said encryption
9 circuit.

84. A token according to claim 1, wherein
2 said token further comprises

0953770.051101

3 a result determination circuit for, when the
4 collation result indicates that the authentication is
5 successful, outputting the authentication data to said
6 encryption circuit, and when the collation result
7 indicates that the authentication fails, outputting the
8 authentication data to said first communication circuit,
9 and

10 an encryption circuit for, in accordance with
11 the authentication data from said result determination
12 circuit, encrypting dynamic information transmitted from
13 the use device using a key registered in advance, adding
14 obtained encrypted data to the authentication data, and
15 outputting the encrypted data, and

16 said communication circuit transmits to the
17 use device the authentication data with the encrypted
18 data from said encryption circuit or the authentication
19 data from said result determination circuit.

85. A token according to claim 1, wherein
2 said token further comprises
3 an encryption circuit for encrypting dynamic
4 information transmitted from the use device using a key
5 registered in advance and outputting obtained encrypted
6 data to said first communication circuit as data, and
7 a first result determination circuit for, when
8 the collation result indicates that the authentication
9 is successful, instructing said encryption circuit to

10 generate the encrypted data, and when the collation
11 result indicates that the authentication fails,
12 outputting data whose number of digits is different from
13 that of the encrypted data to said first communication
14 circuit, and
15 said first communication circuit transmits to
16 the use device the data from said encryption circuit or
17 the data from said first result determination circuit.

86. A token according to claim 84, wherein
2 said token further comprises an ID storage
3 circuit for storing identification information of said
4 authentication token registered in advance, and
5 said first communication circuit transmits to
6 the use device the identification information stored in
7 said ID storage circuit.

87. A system according to claim 10, wherein said
2 storage circuit stores, as the user information,
3 personal information of the user and service information
4 related to the service provided by the use device, and
5 stores the personal information, service information,
6 and registered information in separate storage areas.

88. A system according to claim 10, wherein
2 said authentication token further comprises an
3 encryption circuit for encrypting dynamic information

6 encryption circuit, and when the collation result
7 indicates that the authentication fails, outputting the
8 authentication data to said first communication circuit,
9 and an encryption circuit for, in accordance with the
10 authentication data from said first result determination
11 circuit, encrypting dynamic information transmitted from
12 the use device using a key registered in advance, adding
13 obtained encrypted data to the authentication data, and
14 outputting the encrypted data,

15 said first communication circuit transmits to
16 the use device the authentication data with the
17 encrypted data from said encryption circuit or the
18 authentication data from said first result determination
19 circuit, and

20 said processing unit comprises a dynamic
21 information generation circuit for generating the
22 dynamic information to be transmitted to said
23 authentication token, a decryption circuit for
24 decrypting the encrypted data transmitted from said
25 authentication token using a key corresponding to the
26 key, and a second result determination circuit for
27 causing said decryption circuit to decrypt the encrypted
28 data added to the authentication data only when an
29 authentication result of the authentication data from
30 said authentication token, which is received by said
31 second communication circuit, indicates that the
32 authentication is successful, and executing the

33 predetermined processing only when the obtained dynamic
34 information matches the dynamic information generated by
35 said dynamic information generation circuit and
36 transmitted to said authentication token.

90. A system according to claim 10, wherein

2 said authentication token further comprises an
3 encryption circuit for encrypting dynamic information
4 transmitted from the use device using a key registered
5 in advance and outputting obtained encrypted data to
6 said first communication circuit as data, and a first
7 result determination circuit for, when the collation
8 result indicates that the authentication is successful,
9 instructing said encryption circuit to generate the
10 encrypted data, and when the collation result indicates
11 that the authentication fails, outputting data whose
12 number of digits is different from that of the encrypted
13 data to said first communication circuit,

14 said first communication circuit transmits to
15 the use device the data from said encryption circuit or
16 the data from said first result determination circuit,
17 and

18 said processing unit comprises a dynamic
19 information generation circuit for generating the
20 dynamic information to be transmitted to said
21 authentication token, a decryption circuit for
22 decrypting the encrypted data transmitted from said

23 authentication token using a key corresponding to the
 24 key, and a second result determination circuit for
 25 causing said decryption circuit to decrypt the encrypted
 26 data added to the data only when the number of digits of
 27 the data from said authentication token, which is
 28 received by said second communication circuit, indicates
 29 the number of digits when the authentication is
 30 successful, and executing the predetermined processing
 31 only when the obtained dynamic information matches the
 32 dynamic information generated by said dynamic
 33 information generation circuit and transmitted to said
 34 authentication token.

91. A system according to claim 88, wherein
 2 said authentication token further comprises an
 3 ID storage circuit for storing identification
 4 information of said authentication token registered in
 5 advance,
 6 said first communication circuit transmits to
 7 the use device the identification information stored in
 8 said ID storage circuit, and
 9 said decryption circuit decrypts the encrypted
 10 data from said authentication token using a key
 11 corresponding to the identification information
 12 transmitted from said authentication token.

92. A system according to claim 89, wherein

2 said authentication token further comprises an
3 ID storage circuit for storing identification
4 information of said authentication token registered in
5 advance,

6 said first communication circuit transmits to
7 the use device the identification information stored in
8 said ID storage circuit, and

9 said decryption circuit decrypts the encrypted
10 data from said authentication token using a key
11 corresponding to the identification information
12 transmitted from said authentication token.

93. A system according to claim 90, wherein

2 said authentication token further comprises an
3 ID storage circuit for storing identification
4 information of said authentication token registered in
5 advance,

6 said first communication circuit transmits to
7 the use device the identification information stored in
8 said ID storage circuit, and

9 said decryption circuit decrypts the encrypted
10 data from said authentication token using a key
11 corresponding to the identification information
12 transmitted from said authentication token.